

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-046

29 JAN 1980

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM:
Executive Secretary

SUBJECT: Security Committee

1. With 1979 behind us the accomplishments and shortfalls of the Committee can be appropriately reviewed.

2. The Committee was reorganized and located under your chairmanship in March 1978 in accordance with the Director's desire that adequate resources be dedicated and proper commitments made so as to accomplish much more in security on a Community level than in the past, and that a truly concerted attack be made on policy and implementation discrepancies between the agencies in all major security dimensions.

3. There is reason to believe that a proper commitment by members has been made. Attendance at regular monthly meetings has been regular either by principals or authorized representation. There have been some changes but senior security officers continue to represent their departments or agencies.

4. The Committee held 15 regular meetings and 3 special meetings from its reorganization to the end of 1979. The special meetings covered FOIA, technical security threats, and the report on the investigation.

SECRET

5. The Committee has continued to accept invitations of members. Meetings have been hosted by the Army, where their deputy addressed the committee, by the FBI, where Director Webster addressed the membership, and by NSA, where Deputy Director Robert Drake spoke.

25X1

6. The Committee held a two day seminar to review the applicability and timeliness of basic charter changes, organization problems, progress toward goals and procedural activities.

25X1A

25X1

7. The subcommittees and working groups continue to be alert and move progressively toward accomplishments of charges. They generally meet monthly prior to meetings of the full Committee and reports by their chairmen are regular agenda items.

Subcommittee

Number of Meetings
March 1978 - December 1979

Compartmentation
Chaired by Air Force

7

Computer Security
Chaired by NSA

18

Research & Development
Chaired by CIA

13 plus one
special
meeting

Technical Surveillance Counter-
measures

11

Unauthorized Disclosures
Investigations
Chaired by NSA

1

Working Groups

25X1A

Security Advisory Group USSR
Chaired by State

8

Physical Security Standards
Chaired by Committee staff

7

SECRET

2

SECRET

Working Groups

Number of Meetings
March 1978 - December 1979

Investigative Standards
Chaired by State

7 plus 5 all
day executive
sessions for
drafting of
the SECOM
Personnel
Security
Survey

SCI Denials
Chaired by DIA

5

Security Awareness
Chaired by NSA

20 plus two
special
briefings for
C/SECOM and a
presentation
to the SECOM
Members ☐

25X1

8. The Security Committee has accomplished the following in discharge of responsibilities set for it in its charter - Director of Central Intelligence Directive No. 1/11. ☐ 25X1

9. Mission: Ensure establishment of security policies and procedures including recommendations for legislation for the protection of intelligence and intelligence sources and methods from unauthorized disclosure. ☐ 25X1

10. The Security Committee forwarded to the DCI's General Counsel and Legislative Counsel proposed legislation calling for legal sanctions against leaks and unauthorized disclosures. Significant consideration was given to the Security Committee's proposal but legislative action has been repeatedly postponed and delayed by the Hill in preference to work on an overall legislative package describing and circumscribing lawful limits of activities by the U.S. intelligence community. ☐ 25X1

11. Mission: Review and formulate personnel, physical and document security policies, standards and practices and dissemination procedures applicable to all organizations of the Executive Branch as such policies, standards, practices

SECRET 3

and procedures relate to the protection of intelligence sources and methods in consideration of the effectiveness, risks and cost factors involved. ☐

25X1

12. The SECOM Investigative Standards Working Group was tasked in 1977 to draft common policy guidelines for use in adjudication of investigative data throughout the Intelligence Community. Considerable difficulty was experienced in the drafting process because of different perceptions and beliefs held by members. Drafts were presented to the full Committee in July 1978, November 1978, and unresolved issues were highlighted in the version forwarded to the NFIB in December 1978. The Proposed guidelines were remanded to the Security Committee in July 1979; an amended version was considered by the Committee and released to NFIB in August 1979. The Executive Secretary, NFIB routed the July 1979 version to the DCI General Counsel where it rests as of January 1980. The principal point of contention in the drafting stage related to the treatment of homosexuality. The DCI General Counsel is currently attempting to overcome the NSA position to label the guidelines as optional rather than hard and fast rules. ☐

25X1

13. In January 1979, on behalf of the Security Committee, the Security Awareness Working Group published a bibliography of Security awareness materials which are currently available in the intelligence community. The bibliography was updated in July 1979 and will be updated periodically. Other tasks assigned to the Working Group were the preparation of a Senior Executive Briefing and a Mid-level Professional Briefing, both to be given persons not previously experienced in working with sensitive intelligence sources, methods, and materials. The Senior Executive Briefing was completed in October 1979 and the Mid-level Briefing is in final stages of assembly. The SAWG also prepared a publication on Minimum Security Awareness Programs for Intelligence Community Members. ☐

25X1

14. Following the Boyce-Lee Case, the DCI directed SECOM to establish a method to assure exchange of SCI denial information throughout the Intelligence Community. SECOM assigned the task to the SCI Denials Working Group. After rejecting the idea of a central registry of SCI denials because it appeared to be a "black list," the Working Group proposed and, in September 1979, SECOM approved a set of procedures for exchanging SCI denials information among Intelligence Community members. The SCI Denials Working Group prepared SCI Appeals Procedures to assure due process for persons who have been denied access to SCI. The appeals procedures were concurred in by all but one of the SECOM members. ☐

25X1

15. In connection with physical security the Committee has undertaken a review and update of the 1973 USIB "Uniform Physical Security Standards for the Protection of Sensitive Compartmented Information." This is to capitalize on current state of the art equipment and hardware, modify physical security requirements so as to structure a standard level of protection acceptable to all members of the Community, and to incorporate realistic requirements in view of today's environment. Opportunity is being taken in drafting stages to seek input from the contractor sphere. ☐

25X1

16. In the area of document and information security, the Committee has undertaken the review and update of DCID 1/7 "Control of Dissemination of Foreign Intelligence." A year-long coordination effort was necessary to resolve differences at the SECOM level over such matters as foreign release of intelligence. Efforts to eliminate the NOFORN caveat in favor of policy that intelligence not be released to foreign governments without specific approval were unsuccessful. A draft revision of the DCID was approved by the Committee in November 1979 and sent to the NFIB with DCI approval. ☐

25X1

17. There have been attempts to upgrade personnel security standards for those with access to National Foreign Intelligence. The first such attempt followed on the initiation of the APEX study. Based on the fact that acceptance of APEX would result in the dissemination of a considerable volume of formerly compartmented intelligence at standard levels of classification, an effort was made to require a higher level of clearance standard for all personnel with access to National Foreign Intelligence. The effort was abandoned because of unacceptable cost estimates and the inability of some departments to segregate NFI from the larger volume of classified national security information. It was estimated that if half of the cleared people in DoD needed access to NFI and, if their clearance requirements were at the DoD TOP SECRET level as a condition for access to NFI, the cost would exceed \$176 million. Another approach was to append to E.O. 12065 a standard level of clearance procedures for each level of classification. Thus, personnel nominated for access to Confidential material would have to meet a common clearance criterion; those nominated for access to SECRET level material would have to meet a higher one; and those nominated for TOP SECRET material would be processed through an even more thorough screening. Insufficient interest was evident in the Community to pursue such standards at this time. ☐

25X1

SECRET

25X1 18. The Committee drafted, NFIB approved, and the DCI published DCID 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information," effective 6 June 1978. Subsequent actions have resulted in a committee review of risk areas on a semi-annual basis. ☐

19. Mission: "Review and formulate policies and procedures governing the release of intelligence to foreign governments and international organizations and the review of classified intelligence proposed for release to the public through declassification or other actions..." ☐ 25X1

25X1 20. Committee deliberations on ways and means to govern release to foreign governments and international organizations have been overtaken by events. The Secretary of Defense proposed and the DCI concurred in formation of a senior level group to prepare a National Disclosure Policy on Intelligence similar to the national policy on release of national security information. The DCI's representative to this group has been drawn from his Intelligence Community Collection/Tasking Staff. ☐

Release to the public through declassification or other action has not been addressed by the Committee. ☐ 25X1

25X1 21. Mission: "Ensure that appropriate lawful investigations are made of any unauthorized disclosure or compromise of intelligence or of intelligence sources and methods and that the results of such investigations, along with appropriate recommendations, are provided to the Director of Central Intelligence." ☐

25X1 22. The Committee was briefed on the Lorenzen case in NATO, and is awaiting a report from DIA on whether or not National Foreign Intelligence was compromised. The Security Committee, in recognition of the continued leak problem, elevated the Unauthorized Disclosures Working Group to a subcommittee under NSA Chairmanship, tasked to coordinate in-house investigations toward discovery of sources of leaks. Some difficulty has been experienced due to unanticipated work load encountered by the NSA Chairman in his other job. ☐ 25X1

In a recent case (29 June 1979 NY Times, Richard Burt), Committee members conducted in-house investigations and provided the FBI with results. This action narrowed considerably the scope and detail of investigation required by the FBI and

SECRET

allowed them to concentrate resources in areas outside the NFIB agencies where Committee members could not investigate. Future sharing of investigative requirements and other actions in selection of leaks to be investigated may result in closer Department of Justice cooperation. []

25X1

23. Mission: "Ensure the development, review and use of effective means to defend sensitive U.S. installations or personnel against technical surveillance." []

25X1

24. The Technical Surveillance Countermeasures Subcommittee (TSCS) continues to serve as an active element in providing training, evaluation of equipment, and general information sharing among member departments and agencies. A recently compiled report for the Committee indicates shortfalls in personnel and equipment resources among most member agencies. Finds of technical penetration devices during the past 18 months demonstrate the continued worth of the individual member efforts in this field. []

25X1

An extensive effort by Committee member agencies was undertaken on direction of the DCI to investigate [] While the purpose of [] was not definitively resolved, considerable data was collected and a general agreement reached that [] did not represent a technical threat. []

25X1

25X1



25. Mission: "Review special security and compartmentation procedures and develop proposals for any necessary changes to achieve optimum use of intelligence consistent with protection of sensitive intelligence sources and methods." []

25X1

26. The Committee prepared, and NFIB approved and published DCID 1/19 "Uniform Procedures for Administrative Handling and Accountability of Sensitive Compartmented Information (SCI)," effective 6 June 1978. []

25X1

The Committee Staff was actively engaged in the DCI-directed review and resultant APEX Control System for SCI. Many representatives of the Compartmentation Subcommittee participated as departmental representatives on various panels and working groups associated with APEX. []

25X1

25X1 27. Mission: "Ensure the development, review and maintenance of security standards and procedures for the protection of intelligence stored in or processed by computers." ☐

25X1 28. The Computer Security Subcommittee prepared, the Committee endorsed, and the NFIB approved and issued DCID 1/16, Security of Foreign Intelligence in Automated Data Processing Systems and Networks," effective 6 June 1978. This superseded the May 1976 version and expanded the scope to cover all intelligence information in ADP systems and networks, including SCI. The Computer Security Subcommittee provides the means of sharing and exchanging knowledge about developments in the rapidly changing world of ADP. Review of different systems, and identification of strengths and weaknesses, allows members to better serve in departmental roles for the protection of intelligence stored in or processed by computers. The Subcommittee encounters conflicting interests by virtue of the fact that OMB seeks standards and GSA requires competitive bidding. The intelligence community's security standards for intelligence in ADP programs will continue to be subject to increasing pressures as the Community moves toward more and more networking. ☐

25X1 29. Mission: "Establish and direct an aggressive and imaginative program of research and development leading to improved security equipment and techniques." ☐ 25X1

30. The Committee has endorsed and followed through on several recommendations by its R&D Subcommittee. These ☐ 25X1

☐
investigation were looked at and subsequently tabled because of lack of available funds. Among these are proposals to control unauthorized reproductions, and use of space age technology (metals and ceramics) in new safe and vault construction. ☐ 25X1

31. The DCI's desire for dedication of increased resources to service the Community's security needs have been met with the formation of a small element attached to the Office of the Deputy DCI for Support. Termed the Community Security Group, (CSG) the element consists of seven professional and two clerical positions provided by the CIA. A senior FBI agent and an Air Force Colonel are assigned. The CSG serves as the staff arm of the Security Committee and provides services and coordination to the Subcommittees. The staff has

prepared manuals for administration of the APEX compartmentation system to both government and industry; developed a security plan for U.S. interests in the USSR including proposals for security in the construction of the new U.S. Embassy in Moscow;

[REDACTED]

adjudication standards and SCI appeals procedures; coordinated the DCI's required zero-base review of SCI clearances; coordinated Committee staff papers; reviewed the possibility of upgrading Community personnel security standards for access to National Foreign Intelligence; drafted security procedures for use by the U.S. Foreign Intelligence Surveillance Court; and has served as the Chairman's coordinator and advisor to subcommittees and working groups. In addition, the Group provides security advisors to other NFIB Committees and DCI-directed Community study and working groups as necessary. [REDACTED]

32. In order to meet temporary requirements expeditiously, the Committee has established several working groups. Among these are the Security Advisory Group USSR, Security Awareness Working Group, Investigative Standards Working Group, and the SCI Denials Working Group. They perform specific work in response to tasking from the Chairman and the Committee. The Security Advisory Group--USSR affords Community input and advice to the Department of State related to security matters associated with construction of the new U.S. Embassy and facilities in Moscow. [REDACTED]

33. Current Issues: The Committee presently is addressing the following issues.

a. Revision of its charter, DCID 1/11. A third draft was sent to SECOM members on 31 December 1979. [REDACTED]

b. Refinement and maintenance of the security plan for the new U.S. Embassy in Moscow, particularly in the light of knowledge gained by the Security Advisory Group USSR during their recent trip to the Soviet Union.

[REDACTED]

c. Completing the analysis of the SECOM Personnel Security Survey. [REDACTED]

d. Continuing the review and revision of Community
Physical security standards. ☐

25X1

e. Assessing recommendations on personnel security
by the HPSCI. ☐

25X1



25X1A

Distribution:

Orig - Addressee
1 - C/SECOM
1 - SECOM Subj
1 - SECOM Chrono

25X1A

SECOM: ☐ :kmk (29 Jan 80)

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-063

29 JAN 1980

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM:

[REDACTED]
Executive Secretary

SUBJECT: 30 January Meeting with SCC/CI Working Group

The attached notes may be useful to you as background information in your presentation on personnel security standards to the Working Group.

Attachment

Distribution:

- Orig - Addressee w/att
- 1 - SECOM Chrono w/att
- 1 - SECOM Subject w/att

SECOM/[REDACTED]: fh/kk (1/28/80)

25X1A

Security Processing in the
Intelligence Community

General

- Executive Order 10450 - Civilian employees - "full field" investigation for sensitive positions
- Initially full field was a 15-year background investigation
- Since 1968 some investigative organizations have reduced period to five or seven years due to budgetary constrictions.
- Background Investigations are all similar consisting of record checks and interviews covering individuals' life history, done by trained professional investigators. Some differences in reporting detailed or positive versus short form or negative only.
- Additional authorities for investigation of civilian employees. Statutes, Executive Orders and Directives.

Central Intelligence Agency

- 15-year background Investigation plus polygraph and reinvestigation.

FBI

- Investigation of their own applicants, DOE cases under the Atomic Energy Act, and EO 10450 loyalty investigations.
- Investigation covers entire adult life.
- Also have newly established polygraph program to resolve allegations on a "last resort" type of situation.

Office of Personnel Management

- Conduct background investigations for agencies not having their own investigative capability (such as DOE and Justice) for competitive service employees, plus some for State, Treasury and DOD. Basically a 5-year BI.

Department of State

--7 year BI including an investigative interview (No polygraph).

Department of Treasury

- By agreement with OPM, Treasury conducts its own BI (NACs are conducted by OPM) through investigative arms of the Department, i.e., Secret Service, IRS, Customs, Alcohol, Tobacco and Firearms Bureau, and the Bureau of Printing and Engraving.
- The BI is patterned after OPM's 5-year BI except in cases requiring a DCID 1/14 investigation.
- Polygraph examinations can be conducted on cases related to intelligence positions where there are issues or allegations that cannot be resolved by other means.

Department of Defense

- The Defense Investigative Service conducts investigations for Departments and Agencies of DOD and for Contractor employees with a need for access to classified material.
- Standards are DCID 1/14 (an SBI) for SCI; a 5-year BI or the alternate standard for military personnel (10 years service plus a NAC for access to TS); and NACs for access to Secret or Confidential.
- Only NSA makes use of the polygraph and then only for civilian personnel.

Background Investigation - Polygraph - Reinvestigation

- Combined BI, Polygraph and Reinvestigation result in a sound, comprehensive and continuing personnel security program.
- Examples - NSA's first 100 FPO guards passed Polygraph examinations but 16 were disapproved on OPM investigation.
- 70 NSA military converting to civilian employment had

been approved on DCID 1/14 investigation but when given polygraph, 14 of them were disapproved (Mainly for drug usage).

- The CIA Reinvestigation Program (which includes both an updated background investigation as well as repolygraph) has resulted in serious adverse information, causing the departure of 12 individuals in 1976, 9 individuals in 1977, and 8 individuals in 1978.

Investigative Surveys

- Pilot in 1977.

- 5 Agencies, 1,612 cases to determine the years of coverage necessary to provide an acceptable degree of security assurance and to examine productivity of various sources and determine whether some sources were consistently duplicative.

- Results showed that the following periods of coverage would risk losing data:

	Significant Data	Denial Data
5 years	22%	7%
7 years	19%	5%
10 years	12%	0%

- A separate CIA study of 889 cases in 1977 showed essentially the same results.

- A more comprehensive computerized survey was conducted in 1978-1979 involving more than 5000 cases from 10 agencies of the Intelligence Community.

- confirmed the findings of the Pilot Study.

- Based on data compiled on CIA Polygraph use the survey indicates that the polygraph examination used as a screening device produces far more adverse data and is the source responsible for the highest percentage of security denials.

- At the other end of the scale, sources that produce the

least adverse data are education records checks and certain NACs.

Congressional Studies of Security Clearance Procedures in the Intelligence Community.

- September 1979 HPSCI published report with recommendations which were concerned with the need for greater uniformity in investigative procedures and standards, and a need for improved access to pertinent information. These recommendations are:
 - Standard background investigations needed for access to TS and SCI at the level now required for SCI.
 - Standard investigative reporting needed to insure that positive as well as adverse information is available for adjudicative consideration.
 - Study the use of polygraph to validate its accuracy.
 - Establish Community-wide criteria relating to the use of polygraph.
 - Establish uniform investigative procedures and a centralized office to conduct background investigations for the entire Intelligence Community.
 - Endorse legislation to give Federal investigative agencies access to criminal justice records for background investigations.
 - Resolve the inconsistency between Executive Order 10450, the FBI Guidelines, and the Privacy Act.
- The Security Committee is in agreement with most of the HPSCI recommendations; however, additional resources and legislation will be needed for implementation of all of them.
- GAO report of August 1979 - Cost of Federal Personnel Security Investigations Could and Should Be Cut.
 - Prepared for House Committee on Government Operations and is aimed entirely at cutting costs rather than at assuring effective and informative background investigation report

on which to base decisions effecting the National Security.

--No mention of use of polygraph in the report and it is aimed at EO 10450 considerations rather than protection of sensitive information, methods and sources.